대한민국특허청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2003-0007226
Application Number

출 원 년 월 일 : 2003년 02월 05일
Date of Application FEB 05, 2003

출 원 인 : 학교법인 영광학원
Applicant(s) Foundation of Daegu University

2003 년 11 월 12 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】 명세서 등 보정서

【수신처】 특허청장

【제출일자】 2003.03.06

【제출인】

【명칭】 학교법인 영광학원

【출원인코드】 2-2001-018870-0

【사건과의 관계】 출원인

【대리인】

【성명】 이덕록

【대리인코드】 9-1998-000461-7

【포괄위임등록번호】 2001-026439-3

【사건의 표시】

【출원번호】 10-2003-0007226

【출원일자】 2003.02.05

【심사청구일자】 2003.02.05

【발명의 명칭】 유한 필드 GF(2m)상의 산술연산기

【제출원인】

【접수번호】 1-1-03-0040411-85

【접수일자】 2003.02.05

【보정할 서류】 명세서등

【보정할 사항】

【보정대상항목】 별지와 같음

【보정방법】 별지와 같음

【보정내용】 별지와 같음

【취지】 특허법시행규칙 제13조·실용신안법시행규칙 제8조의 규정에의하여 위와 같 이 제출합니다. 대리인
이덕록 (인)

【수수료】

【보정료】 0 원

【추가심사청구료】 0 원

【기타 수수료】 0 원

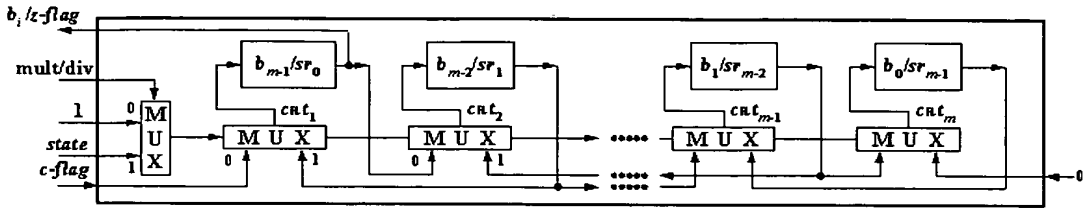
【합계】 0 원

【보정대상항목】 도 6

【보정방법】 정정

【보정내용】

【도 6】

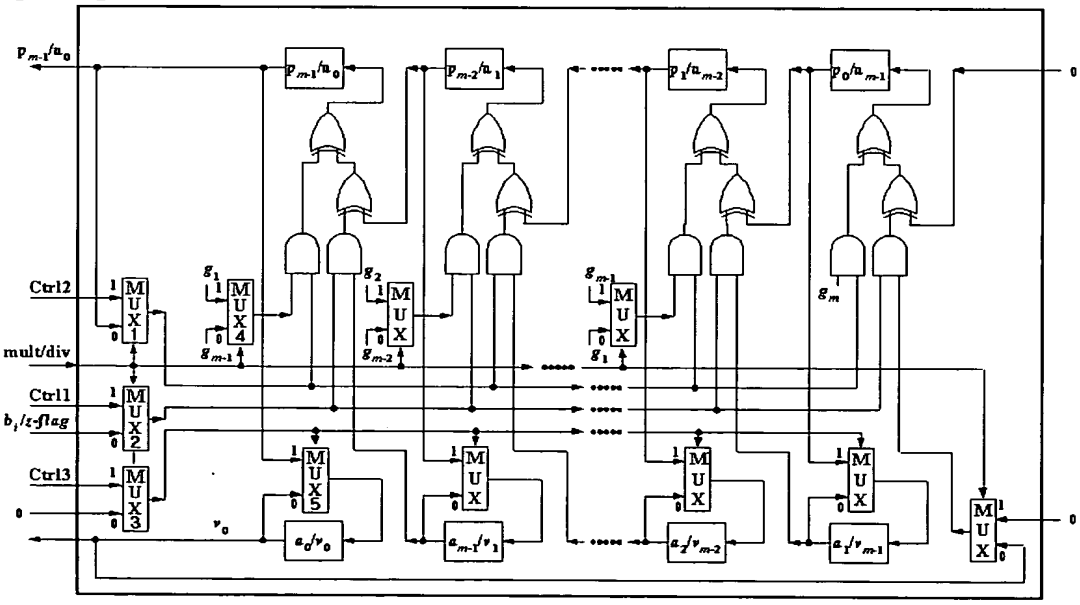


【보정대상항목】 도 7

【보정방법】 정정

【보정내용】

【도 7】



【보정대상항목】 도 8

【보정방법】 삭제

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【제출일자】	2003.02.05
【발명의 명칭】	유한 필드 GF(2m)상의 산술연산기
【발명의 영문명칭】	Arithmetic unit over finite field GF(2m)
【출원인】	
【명칭】	학교법인 영광학원
【출원인코드】	2-2001-018870-0
【대리인】	
【성명】	이덕록
【대리인코드】	9-1998-000461-7
【포괄위임등록번호】	2001-026439-3
【발명자】	
【성명의 국문표기】	홍춘표
【성명의 영문표기】	HONG,Chun Pyo
【주민등록번호】	560830-1803017
【우편번호】	712-714
【주소】	경상북도 경산시 진량읍 내리리 15번지 대구대학교 정보통신공학부
【국적】	KR
【발명자】	
【성명의 국문표기】	김창훈
【성명의 영문표기】	KIM,Chang Hoon
【주민등록번호】	760215-1836411
【우편번호】	712-714
【주소】	경상북도 경산시 진량읍 내리리 15번지 대구대학교 정보통신공학부
【국적】	KR
【심사청구】	청구
【취지】	특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인 이덕록 (인)

【수수료】

【기본출원료】	14	면	29,000 원
【가산출원료】	0	면	0 원
【우선권주장료】	0	건	0 원
【심사청구료】	1	항	141,000 원
【합계】	170,000 원		
【감면사유】	학교		
【감면후 수수료】	85,000 원		

【첨부서류】 1. 고등교육법 제2조에의한 학교임을 증명하는 서류_1통

【요약서】

【요약】

본 발명은 유한필드 GF(2^m)상에서의 산술연산기에 관한 것으로, 바이너리 확장 최대공약수 알고리즘에 바탕을 둔 나눗셈 알고리즘과, MBS(Most Significant Bit)-first 곱셈 알고리즘으로부터 구현한 산술연산기는 하드웨어 공유를 통하여 곱셈 및 나눗셈 모두를 수행할 수 있고, 본 발명 연산기는 기약다항식의 선택에 어떠한 제약도 두지 않을 뿐 아니라 매우 규칙적이고 모듈화하기 쉽기 때문에 필드 크기 m 에 대하여 확장성 및 유연성을 가지며 곱셈 및 나눗셈 연산을 동일한 하드웨어로 수행할 수 있기 때문에 스마트 카드나 무선통신기기와 같은 저 면적을 요구하는 응용들의 암호화 시스템 구현에 적합한 매우 뛰어난 발명인 것이다.

【대표도】

도 3

【색인어】

유한필드, 산술연산기, 곱셈, 나눗셈, 하드웨어, 알고리즘, 바이너리 확장 최대공약수, MBS-first 곱셈 알고리즘

【명세서】

【발명의 명칭】

유한 필드 G F(2m)상의 산술연산기 {Arithmetic unit over finite field G F(2m)}

【도면의 간단한 설명】

도 1은 본 발명의 바람직한 실시예에 따른 MSB(Most Significant Bit)-first 곱셈 알고리즘,

도 2는 본 발명의 바람직한 실시예에 따른 나눗셈 알고리즘,

도 3은 본 발명은 바람직한 실시예에 따른 곱셈 및 나눗셈을 모두 수행하는 산술연산기의 블록도,

도 4는 상기 도 1의 컨트롤 로직부의 내부 회로도,

도 5는 상기 도 1의 RS-블록부의 회로도,

도 6은 상기 도 1의 SR-블록부의 회로도,

도 7은 상기 도 1의 UV-블록부의 회로도이다.

* 도면의 주요부분에 대한 부호의 설명 *

1 : 컨트롤 로직부 2 : 알에스-블록부

3 : 에스알-블록부 4 : 유브이-블록부

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<11> 본 발명은 유한필드 GF(2^m)상에서의 산술연산기에 관한 것으로 더욱 상세하게는 바이너리 확장 최대공약수 알고리즘에 바탕을 둔 나눗셈 알고리즘과 MSB(Most Significant Bit)-first 곱셈 알고리즘으로부터 하드웨어 공유를 통하여 한 개의 동일한 하드웨어를 이용하여 곱셈 및 나눗셈 모두를 수행하는 유한필드 GF(2^m)상에서의 산술연산기에 관한 것이다.

<12> 종래의 곱셈 및 연산기는 출원번호 특허 1995-22327호에 공지된 바와 같이 곱셈 및 나눗셈 연산용 지원회로는 인가되는 데이타를 저장하기 위한 제1,2레지스터와; 상기 제2레지스터의 출력을 멀티플렉싱하는 제1멀티플렉서와; 상기 제1레지스터와 상기 제1멀티플렉서의 출력을 수신하고 인가되는 산술제어신호에 따라상기 수신된 출력을 산술연산하는 논리산술 연산기와; 상기 논리산술 연산기의 출력을 수신하여 곱셈 및 나눗셈을 위한좌우 시프팅을 행하고 상기 산술제어신호를 제공하는 병렬 리드 및 라이트 가능한 시프트 레지스터와; 상기 논리산술 연산기와 연결되어 네가티브 플래그 및 오버플로우 플래그를 게이팅하여 그 결과를 출력하는 게이트와; 상기 논리산술 연산기의 출력과 상기 게이트의 출력 및 상기 제1멀티플렉서의 출력을 수신하여 멀티플렉싱하는 제2멀티플렉서를 포함하는 곱셈 및 나눗셈 지원회로가 있었다.

<13> 도 1 및 도 2에 도시된 알고리즘은 각각 곱셈 및 나눗셈을 위한 것으로 지금까지 연산기는 곱셈만을 위한 구조 또는 나눗셈만을 위한 구조로 구분되어 있었으며, 본 발명과 같이 한 개의 동일한 하드웨어를 이용하여 곱셈 및 나눗셈 모두를 수행하지 못하는 문제점이 있었다.

<14> 따라서, 본 발명은 상기 문제점을 해결하기 위해서 안출된 것으로 본 발명의 목적은 한 개의 동일한 하드웨어를 이용하여 유한필드 GF(2^m)상에서의 곱셈 및 나눗셈 모두를 수행할 수 있는 기능을 가진 산술연산기를 제공하는데 있다.

【발명이 이루고자 하는 기술적 과제】

<15> 본 발명은 상기 언급한 문제점을 감안하여 안출한 것으로서, 본 발명의 목적은 도 1의 곱셈 및 도 2의 나눗셈 알고리즘을 수행할 수 있는 산술연산기를 개발하는 것이며, 컨트롤 로직과, RS-블록, SR-블록, UV-블록의 4개 구성요소로 이루어짐으로써 GF(2^m)상의 곱셈 및 나눗셈을 모두 수행하는 하는 기능을 가짐으로써 본 발명의 목적을 달성하였다.

【발명의 구성 및 작용】

<16> 이하, 본 발명의 바람직한 실시예로서 첨부된 도면에 의거하여 상세히 설명한다.

<17> 도 1은 본 발명의 바람직한 실시예에 따른 곱셈 알고리즘이고, 도 2는 본 발명의 바람직한 실시예에 따른 나눗셈 알고리즘으로서, 각각의 알고리즘을 실행할 수 있는 각각의 곱셈기 및 나눗셈기를 설계하여 그 구조를 분석한 결과 하드웨어의 공유가 가능하다는 사실을 인지하였으며, 본 발명은 이 결과를 종합한 것으로서 한 개의 동일한 하드웨어를 이용하여 GF(2^m)상의 곱셈 및 나눗셈 모두를 수행할 수 있는 기능을 가진 산술연산기를 설계한 것이다.

<18> 도 3은 본 발명은 바람직한 실시예에 따른 곱셈 및 나눗셈을 동시에 수행하는 연산기의 블록도로 컨트롤 로직부(1), RS-블록부(2), SR-블록부(3), UV-블록부(4)로 구성되어 있으며 상기

컨트롤 로직부(1), RS-블록부(2), SR-블록부(3), UV-블록부(4)는 하기 도 4 내지 도 7에서 상세히 설명한다.

<19> 도 4는 상기 도 1의 컨트롤 로직부(1)의 내부 회로도로 입력값 R_0와, 입력값 state가 NOT Gate를 통해 상기 입력값 R_0와 같이 AND Gate의 출력값1을 출력하고 입력값 state와, 입력값 z-flag가 인버터를 통해 상기 입력값 state와 같이 AND Gate의 출력값2를 출력하여 상기 출력값1과 함께 OR Gate에 입력되어 출력값 state를 만드는 회로와; 입력값 z-flag값과, state값이 AND Gate를 통해 c-flag의 출력값을 만드는 회로와; 입력값 R_0, V_0가 AND Gate를 통해 출력값3을 만들고 입력값 U_0와 함께 XOR Gate의 입력값이 되어 출력 Ctrl2를 만드는 회로와; 입력값 R_0와, 입력값 state가 인버터 회로를 통해 상기 입력값 R_0와 함께 AND Gate회로를 통해 출력값 Ctrl3를 만드는 회로로 구성되어 있는 컨트롤 로직 회로이다.

<20> 상기 컨트롤 로직 회로는 RS-블록부(2), SR-블록부(3), UV-블록부(4)에 필요한 제어신호를 생성하는 작용을 한다.

<21> 도 5는 상기 도 1의 RS-블록부(2)의 회로도로 상기 도 4에 도시된 컨트롤 로직부(1) 회로에서 출력값 Ctrl1, Crrl3는 RS-블록 회로도의 입력값으로 들어가 출력값 r_0를 출력한다. 상기 RS-블록의 세부 회로를 살펴보면 입력값 r_1은 XOR Gate의 입력값과, MUX 논리회로의 입력값으로 되고 상기 MUX는 입력값 r_1, Ctrl3, S_1가 입력값이 되어 출력값을 생성하고 이 출력값은 다시 S_1 입력값이 되고 AND Gate 회로의 입력값으로 들어간다. 그리고 상기 AND Gate 회로는 S_1의 출력값이 다시 입력값이 되어 Ctrl1의 입력값과 함께 AND Gate에 들어가 출력값을 생성한다. 이렇게 생성된 출력값은 상기 입력값 r_1과 함께 XOR- Gate의 입력값이 되어 출력값 r_0을 생성한다.

<22> 상기 r과 s는 1-bit 레지서터를 나타내고 있으며 상기 MUX는 2-input 멀티플렉서를 나타내고 있다. 상기 RS-블록은 도 1에 도시된 종래의 알고리즘에서 R 및 S 값을 계산하는 기능을 가지고 또한 R_0 값을 컨트롤 로직부(1)로 전송하는 작용을 한다.

<23> 도 6은 상기 도 1의 SR-블록부(2)의 회로도로 MUX논리 회로에 입력값 1, state, mult/div가 입력되어 출력값을 생성하고 이렇게 생성된 출력값은 cnt1 MUX의 입력값으로 상기 MUX의 출력값, c-flag, b_{m-2}/sr_1와 함께 입력되어 출력값 b_{m-1}/sr_0를 생성하여 다음 cnt2 MUX논리회로의 입력값으로 입력된다. 상기와 같은 회로동작을 반복하는 SR-블록부(3) 회로인 것이다.

<24> 그리고 b_i/sr_i는 1-bit 레지서터를 나타내고 있으며 MUX는 2-input multiplexer를 나타내고 있으며 여기서 연산기가 곱셈연산을 수행하는 경우에는 state 값이 항상 1이기 때문에 레지스터의 값이 왼쪽 방향으로만 이동된다. 만약 연산기가 나눗셈 연산을 수행하는 경우는 state 값에 따라 레지스터의 값이 왼쪽 또는 오른쪽 방향으로 이동한다.

<25> 도 7은 상기 도 1의 UV-블록부(4)의 회로도로 두 개의 AND Gate 회로에 입력되는 입력값은 MUX4의 입력값 g1, g_{m-1}, mult/div에 의해서 나온 출력값과, 입력값 Ctrl2, p_{m-1}/u_0, mult/div가 MUX에 입력되어 출력된 값이 제 1 AND Gate의 입력값이 되고, 제 2 AND Gate의 입력값은 Ctrl1, b_i/z-flag, mult/div가 MUX2에 입력되어 출력된 값과, a_{m-1}/v_1가 입력되어 출력한다.

<26> 한편, 두 개의 XOR Gate 중에서 제 1 XOR Gate는 상기 제 1 AND Gate의 출력값이 입력값이 되고 제 2 XOR Gate는 입력값 p_{m-2}/u_1와, 상기 제 2 AND Gate의 출력값이 입력값이 되어 출력하고 이렇게 출력된 출력값은 상기 제 1 AND Gate의 출력값과 같이 제 1 XOR Gate의 입력값이 되어 p_{m-1}/u_0의 출력값을 출력한다.

<27> 상기 p_{m-1}/u_0는 다시 MUX5의 입력값이 되고 MUX5의 입력값은 입력값 Ctrl3, 0가 MUX3에 들어가 출력된 값과, 상기 P_{m-1}/u_0 값, a_0/v_0가 입력되어 출력값을 생성한다. 또한 출력된 값은 a_0/v_0에 입력되어 a_0/v_0를 출력하고 MUX에 재 입력된다.

<28> 상기 p_i/sr_i 및 ai/vi는 1-bit 레지스터를 나타내고 있으며 MUX는 2-input multiplexer를 나타낸다. 이 RS-블록은 기본적으로 도 1에 도시된 알고리즘에서 U 및 V 값을 계산하는 기능을 가진다. 또한 p_i/sr_i 값 및 a_i/vi 값을 상기 도 4의 컨트롤 로직으로 전송해주는 작용을 한다.

<29> 이상 설명한 바와 같이 표 1은 본 발명과 종래의 곱셈 및 나눗셈 장치를 비교 한 것이다.

<30> [표 1]

<31> 기존의 나눗셈기와 본 발명 연산기의 성능 비교표

<32>

	Brunner	Guo	본 발명의 연산기
처리량(1/cycles)	1/2m	1/m	1/2m-1
계산지연시간(cycles)	2m	5m-4	2m-1
최대 처리기 지연시간	Tzero - detector + $2T_{AND2}$ + $2T_{XOR}$ + $2T_{MUX2}$	T_{AND2} + $3T_{XOR2}$ + T_{MUX2}	$2T_{AND2}$ + $3T_{XOR2}$ + T_{XOR2}
회로의 구성요소들	AND_2 : 3m + $\log_2(m+1)$ XOR_2 : 3m + $\log_2(m+1)$ FF : 4m + $\log_2(m+1)$ MUX_2 : 8m	AND_2 : 16m -16 XOR_2 : 10m -10 FF : 44m -43 MUX_2 : 22m - 22	AND_2 : 3m + 7 XOR_2 : 3m + 1 OR_2 : 2 FF : 5m + 2 MUX_2 : 3m + 2
트랜지스터 개수	110m + 18log2(m +1)	608m - 432	88m + 84
수행연산	나눗셈	나눗셈	곱셈/나눗셈

<33> AND_i : i-input AND gate

<34> XOR_i : i-input XOR gate

<35> OR_i : i-input OR gate

<36> MUX_i : i-to-1 multiplexer

<37> T_{ANDi} : 한 개 AND_i gate를 통한 전송지연 시간

<38> T_{XORi} : 한 개 XOR_i gate를 통한 전송지연 시간

<39> T_{MUXi} : 한 개 MUX_i gate를 통한 부동지연 시간

<40> Tzero-detector : log2(m +1)-bit zero-detector의 전송지연 시간

【발명의 효과】

<41> 이상 설명한 바와 같이, 본 발명은 나눗셈기 기능만을 기존의 나눗셈기들과 비교 분석한 결과, 계산 지연시간이 감소될 뿐만 아니라 하드웨어 구현을 위한 트랜지스터의 개수도 감소되었고 지금까지 유한필드 GF(2^m)상의 연산기 구현을 위해서 독립된 곱셈 및 나눗셈 모듈을 사용했지만, 본 발명을 이용하면 별개의 곱셈 및 나눗셈 모듈을 사용할 필요가 없는 효과가 있으므로 스마트 카드나 무선 통신기기와 같은 저 면적을 요구하는 응용들의 암호화 시스템 구현에 매우 적합하고 필드 크기 m 에 대하여 높은 확장성 및 유연성을 가지기 때문에 유한필드 GF(2^m)상의 산술연산기로 다양하게 활용되는 효과가 있으므로 암호화 시스템을 이용하는 장치산업상 매우 유용한 발명인 것이다.

【특허청구범위】

【청구항 1】

출력값 r_0 값을 컨트롤 로직부(1)에 전송하고 알고리즘의 R과 S의 값을 계산하는 RS-블록부(2)와; 곱셈 및 나눗셈 연산을 수행하여 레지스트값이 오른쪽 및 왼쪽으로 이동하는 SR-블록부(3)와; pi/sri 값 및 ai/vi 값을 컨트롤 로직부(1)로 전송하고 알고리즘의 U와 V값을 계산하는 UV-블록부(4)와; 곱셈 및 나눗셈을 동일한 하드웨어로 수행하도록 상기 RS-블록부(2), SR-블록부(3), UV-블록부(4)에 필요한 제어신호를 생성하는 컨트롤 로직부(1)로 이루어진 것을 특징으로 하는 곱셈 및 나눗셈을 동시에 수행하는 연산기.

【도면】

【도 1】

MSB-first Multiplication algorithm Over GF(2^m)

Input : $A(x)$, $B(x)$, $G(x)$
Output : $P(x)=A(x)B(x)$ *mod* $G(x)$
1. $a_k^{(0)}=a_k$, for $0\le k\le m-1$
2. $a_{-1}^{(i)}=0$, for $1\le i\le m$
3. $p_k^{(0)}=0$, for $0\le k\le m-1$
4. for i = 1 to m do
5. for k = $m-1$ down to 0 do
6. $a_k^{(i)}=a_{k-1}^{(i-1)}+a_{m-1}^{(i-1)}g_k$
7. $p_k^{(i)}=a_k^{(i-1)}b_{i-1}+p_k^{(i-1)}$
8. end
9. end
10. $P(x)$ = $p^m(x)$

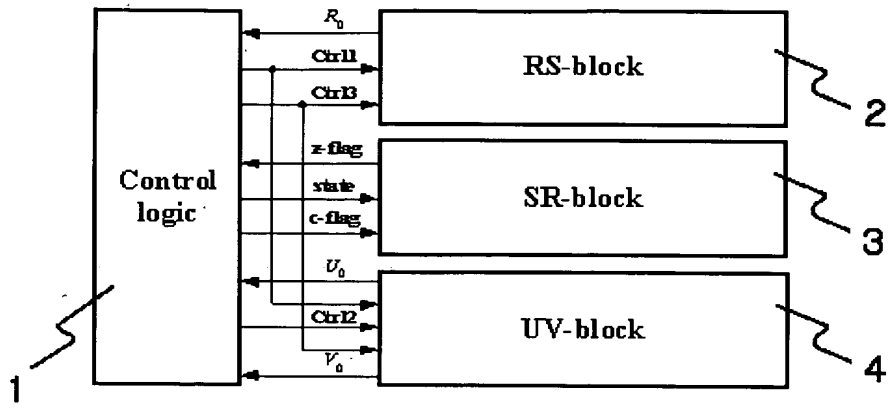
【도 2】

New Division Algorithm Over GF(2^m) for VLSI Implementation

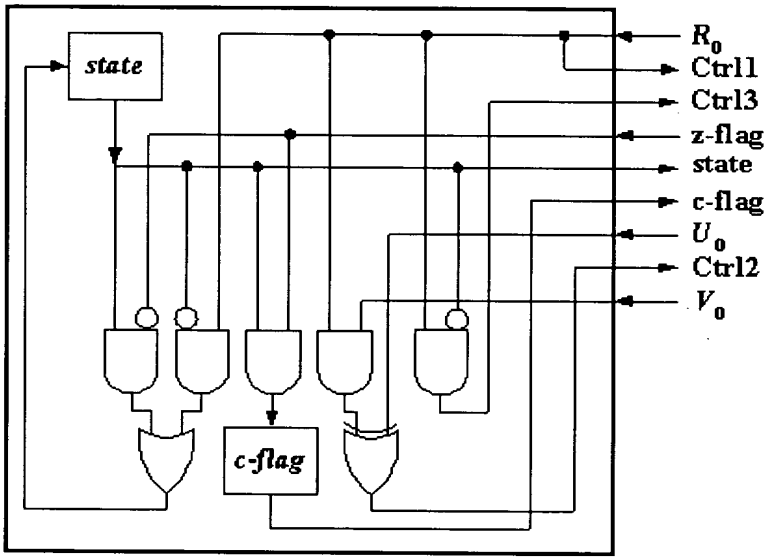
Input: $G(x)$, $A(x)$, $B(x)$
Output: V has $P(x)=A(x)/B(x)$ mod $G(x)$
Initialize: $R=B(x)$, $S=G=G(x)$, $U=A(x)$, $V=0$, *count*=0, *state*=0

```
1.  for i = 1 to 2m do
2.      if state == 0 then
3.        count = count+1;
4.        if r0 == 1 then
5.          (S, R)=(R, R+S); (V, U)=(U, U+V);
6.          state = 1;
7.        end if
8.      else
9.        count = count-1;
10.       if r0 == 1 then
11.         (S, R)=(S, R+S); (V, U)=(V, U+V);
12.       end if
13.       if count == 0 then
14.         state = 0;
15.       end if
16.     end if
17.     R = R/x;
18.     if u0 == 0 then
19.       U = U/x;
20.     else
21.       U = (U+G)/x;
22.     end if
23. end for
```

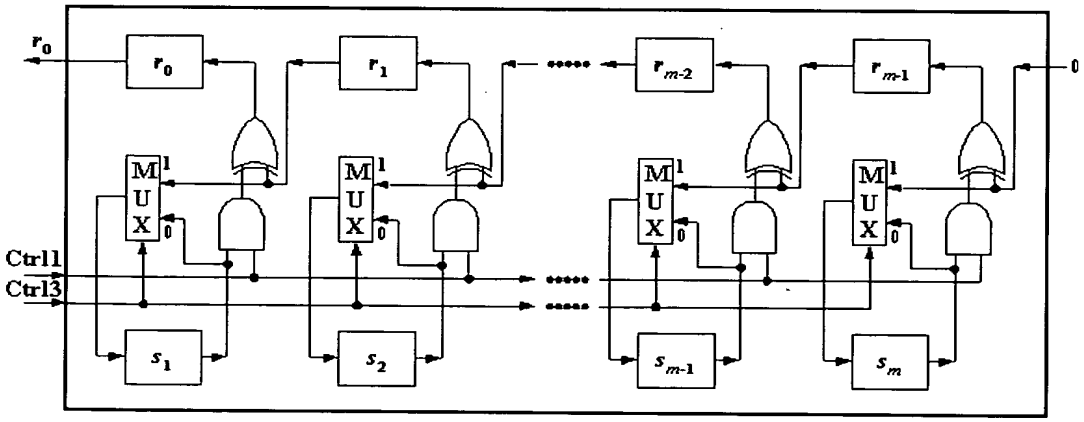
【도 3】


Control logic
RS-block
SR-block
UV-block
Ctrl1
Ctrl3
z-flag
state
c-flag
Ctrl2
1
2
3
4

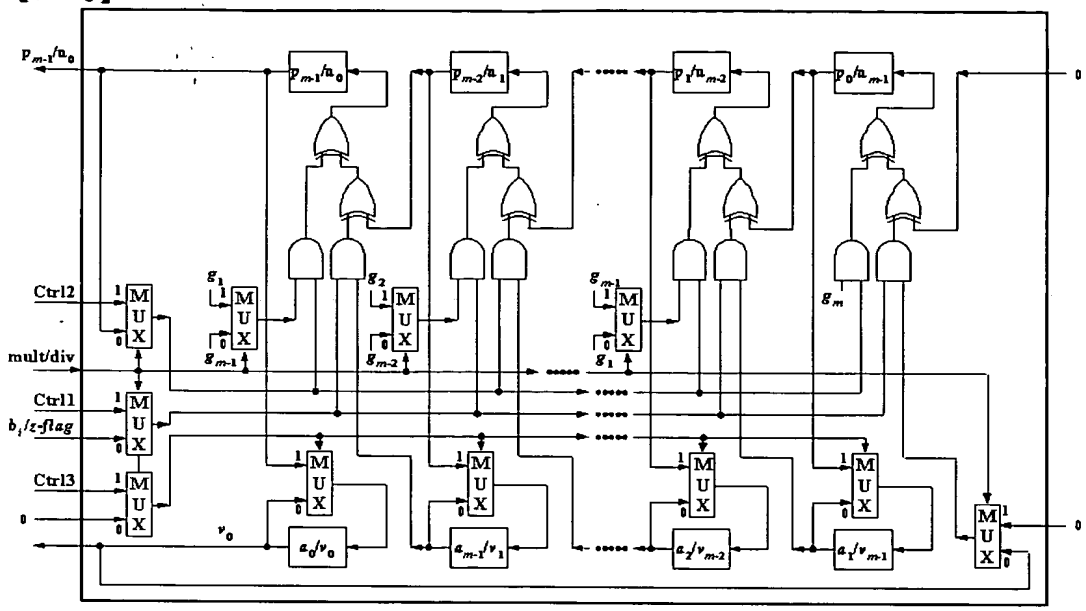
【도 4】


state
c-flag
Ctrl1
Ctrl3
z-flag
state
c-flag
Ctrl2

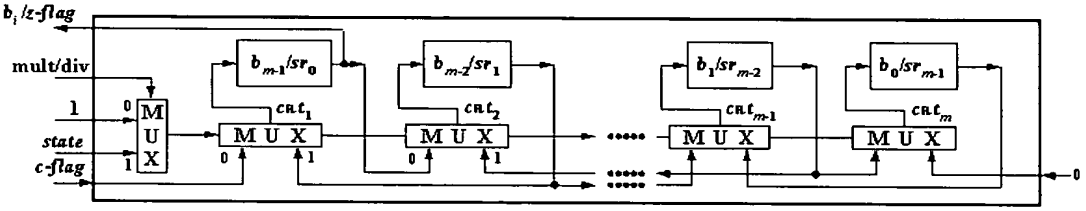
【도 5】


MUX
Ctrl1
Ctrl3

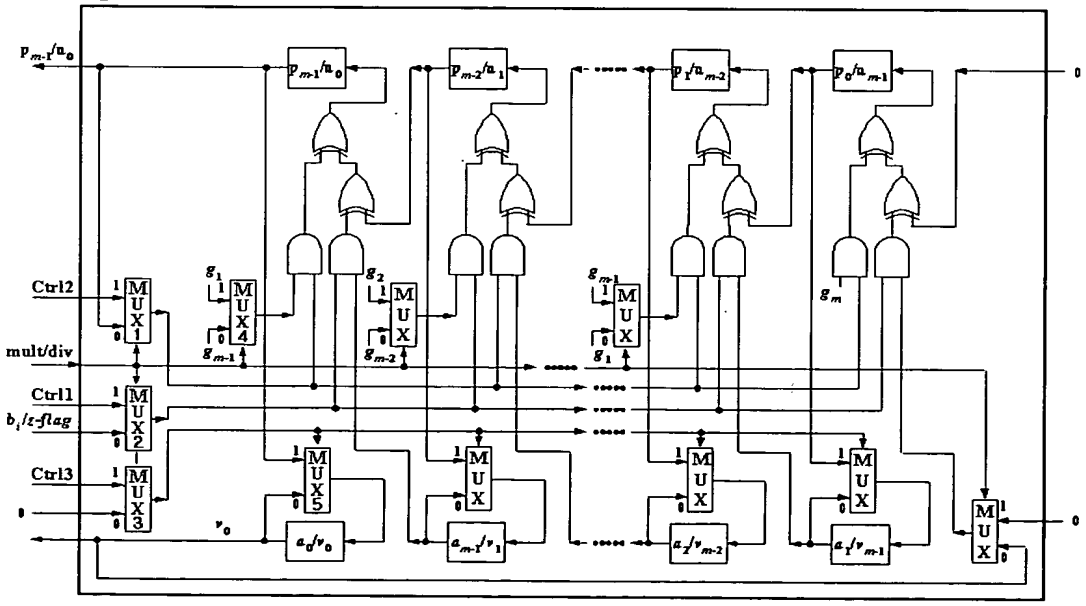
【도 6】


Ctrl2
mult/div
Ctrl1
Ctrl3
MUX

【도 7】


mult/div
1
state
c-flag
MUX

【도 8】


Ctrl2
mult/div
Ctrl1
Ctrl3
MUX